【명세서】

【발명의 명칭】

디지털 컨텐트 무단 복제 방지 시스템{System for protecting copy of digital contents}

【도면의 간단한 설명】

도 1은 본 발명인 디지털 컨텐트 무단 복제 방지 시스템을 설명하기 위한 개략적인 도면,

도 2에서 도 5은 도 1에 적용된 각 블록들이 등록요청 또는 디지털 컨텐트를 재생시키고자 하는 경우에 대해 간단히 설명하기 위한 도면이고,

도 6은 본 발명이 지원하는 파일 포맷의 일 예를 도시한 도면,

도 7은 본 발명에 부가적으로 연결될 수 있는 출력소오스를 도시한 도면,

도 8는 도 7의 출력소오스를 지원하기 위한 입력 제어 블록도를 도시한 도면이다.

도면의 주요부분에 대한 부호설명

10 : 권한부여수단

20 : 휴대 단말기 공급수단

30 : 컨텐트 공급수단

40 : PC

50 : 휴대용 단말기

60 : 저장매체

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

본 발명은 디지털 컨텐트 무단 복제 방지 시스템에 관한 것이다.

보다 상세하게는 사용자가 재생하고자 다운받은 암호화된 디지털 컨텐트가 무단 복제되는 것을 방지하기 위해 사용자와 연결되는 모든 시스템이 서로 상호간에 공유할 수 있는 다수의 키를 생성하여 공유하고, 상호간에 형성된 시크리트 채널를 이용하여 디지털 컨텐트를 다운로드 또는 업로드하는 디지털 컨텐트 무단 복제 방지 시스템에 관한 것이다.

최근 통신환경이 급속도로 발전하고, 각 개인이 통신장비가 구비된 PC를 가지고 있으며, 이 PC를 여러 가지 정보를 접할 수 있게 되었다.

그러므로 상술한 PC에 좀더 많은 디지털 정보를 제공하고자 하는 디지털 컨텐트 공급자들이 존재하게 되었다. 상술한 디지털 컨텐트는 단순한 문서 정보뿐만 아니라 MP3와 같은 오디오 파일도 있다.

대부분 디지털 컨텐트 공급업체는 디지털 컨텐트를 제공함에 있어 소정의 요금이 지불되도록 하고 있다.

그러나, 상술한 바와 같이 종래 기술에서는 사용자에게 한번 제공된 디지털 컨테트가 무단 복제되는 경우 디지털 컨텐트 공급자가 이를 방지하기 어렵다는 문제점이 있었다.

본 발명은 무단 복제를 방지하기 위한 휴대용 저장매체를 갖는 시스템에 관한 것이다.

보다 상세하게는 휴대용 저장매체 제조시 발생되는 불량섹터의 물리적 주소를 이용하여 휴대용 저장매체에 저장되는 암호화된 디지털 컨텐트의 헤더를 다시 암호화시켜 휴대용 단말기를 통해 다운로드받은 디지털 컨텐트를 저장매체를 통해 불법으로 복제할 수 없도록 하는 무단 복제를 방지하기 위한 휴대용 저장매체를 갖는 시스템에 관한 것이다.

최근 통신환경이 급속도로 발전하고, 각 개인이 통신장비가 구비된 PC를 가지고 있으며, 이 ~~PCLCM~~를 여러 가지 정보를 접할 수 있게 되었다.

그러므로 상술한 ~~PCLCM~~에 좀더 많은 디지털 정보를 제공하고자 하는 디지털 컨텐트 공급자들이 존재하게 되었다. 상술한 디지털 컨텐트는 ~~단순한 문서 정보뿐만 아니라 MP3와 같은 오디오 파일도 있다~~**Audio/Video 정보뿐만 아니라 음악가사, 영화자막 등의 문자정보도 있다.**.

상술한 디지털 컨텐트는 ~~PCLCM~~뿐만 아니라 ~~MP3(MP3로 국한 시키지 말것. MP3 말고도 AAC, G2등 많음. 저희 제안은 여러종류의 Codec을 지원함.)~~플래이어인 휴대용 단말기에 다운로드받아 재생시킬 수 있다. 그리고 휴대용 저장매체를 통해 다운로드받아 다른 휴대용 단말기에 장착시켜 재생시킬 수 있다.

이때, 휴대용 저장매체는 ~~스마트 미디어 (스마트미디어로 국한 시키지 말것) 매체로서~~ 데드 카피를 하게 되는 경우, 디지털 컨텐트가 불법으로 복제된다는 문제점이 있었다.

【발명이 이루고자하는 기술적 과제】

따라서, 본 발명의 목적은 전술한 문제점을 해결할 수 있도록 사용자가 재생하고자 다운받은 암호화된 디지털 컨텐트가 무단 복제되는 것을 방지하기 위해 사용자와 연결되는 모든 시스템이 서로 상호간에 공유할 수 있는 다수의 키를 생성하여 공유하고, 상호간에 형성된 시크리트 채널를 이용하여 디지털 컨텐트를 다운로드 또는 업로드하는 디지털 컨텐트 무단 복제 방지 시스템을 제공함에 있다.

따라서, 본 발명의 목적은 전술한 문제점을 해결할 수 있도록 휴대용 저장매체 제조시 발생되는 불량섹터의 물리적 주소를 이용하여 휴대용 저장매체에 저장되는 암호화된 디지털 컨텐트의 헤더를 다시 암호화시켜 휴대용 단말기를 통해 다운로드받은 디지털 컨텐트를 저장매체를 통해 불법으로 복제할 수 없도록 하는 무단 복제를 방지하기 위한 휴대용 저장매체를 갖는 시스템을 제공함에 있다.

【발명의 구성 및 작용】

이와 같은 목적을 달성하기 위한 본 발명은, 암호화된 디지털 컨텐트를 공급하거나, 또는 공급받아 재생, 출력할 수 있도록 제조키 및 제조키 정보를 생성, 송출하고, 디지털 컨텐트를 제공할 수 있는 인증 자격 키 및 그 키정보를 암호화하여 송출하는 권한부여수단과, 권한부여수단으로 등록 요청신호를 송출하고, 등록 요청신호에 의해 발생된 제조키 및 제조키 정보를 전송받는 휴대용 단말기 공급수단과, 권한부여수단으로 등록 요청신호를 송출하고, 등록 요청신호에 의해 발생된 암호화된 디지털 컨텐트를 제공할 수 있는 자격을 부여하기 위해 권한부여수단에서 생성된 한쌍의 키와 그 키정보를 전송받는 컨텐트 공급수단과, 컨텐트 공급수단에서 공급하는 디지털 컨텐트를 공급받아 재생, 출력시키고자 등록 요청신호를 컨텐트 공급수단으로 송출하고, 상기 등록 요청신호에 의해 발생된 퍼블릭키와 퍼블릭키 정보 및 디지털 컨텐트를 공급받을 수 있도록 암호화된 한쌍의 키와 그 키정보를 전송받는 PC를 포함한다.

또한, 상술한 목적을 달성하기 위한 본 발명은, 암호화된 디지털 컨텐트를 공급하거나, 또는 공급받아 재생, 출력할 수 있도록 제조키, 제조키 정보 및 상기

제조키와 제조키 정보를 갖는 제 1 테이블을 형성하고, 상기 테이블과 한쌍으로 휴대용 단말기의 ID, 제조키로 토큰을 암호화시킨 정보, 토큰을 갖는 제 2 테이블을 형성하고, 휴대용 단말기로 디지털 컨텐트를 공급할 수 있도록 하는 한쌍의 자격 인증 키 및 자격 인증 키정보를 생성하여 송출하는 권한부여수단과, 권한부여수단으로 등록 요청신호를 송출하고, 등록 요청신호에 의해 발생된 제조키 및 제조키 정보를 전송받는 휴대용 단말기 공급수단과, 권한부여수단으로 등록 요청신호를 송출하고, 등록 요청신호에 의해 발생된 암호화된 디지털 컨텐트를 제공할 수 있는 자격이 부여되는 한쌍의 키와 그 키정보를 전송받고, 상기 권한부여수단의 제 2 테이블을 전송받는 컨텐트 공급수단과, 컨텐트 공급수단에서 공급하는 디지털 컨텐트를 공급받아 재생, 출력시키고자 등록 요청신호를 컨텐트 공급수단으로 송출하고, 상기 등록 요청신호에 의해 발생된 Public Key와 Public Key 정보를 전송받고, 제조키 정보를 컨텐트 공급수단을 바이패스시키며, 제 2 테이블로부터 상기 제조키 정보에 해당되는 테이블 정보를 검출하여 암호화한 후 전송하는 PC와, 권한부여수단에서 전송하는 제조키 및 제조키 정보를 입력받아 저장하고, PC를 통해 컨텐트 공급수단으로 제조키 정보를 송출하며, 상기 PC에서 전송되는 자신에게 해당하는 암호화된 제 2 테이블의 제조키 정보를 입력받는 휴대용 단말기를 포함한다.

이하, 첨부한 도면들을 참조하여 본 발명의 바람직한 실시 예를 상세히 기술하기로 한다.

도 1은 본 발명인 디지털 컨텐트 무단 복제 방지 시스템을 설명하기 위한 개략적인 도면으로서, 도시된 바와 같이 그 구성은 다음과 같다.

권한부여수단(10)은 암호화된 디지털 컨텐트를 공급하거나, 또는 공급받아 재생, 출력할 수 있도록 제조키, 제조키 정보 및 상기 제조키와 제조키 정보를 갖는 제 1 테이블을 형성하고, 상기 테이블과 한쌍으로 휴대용 단말기의 ID, 제조키로 토큰을 암호화시킨 정보, 토큰을 갖는 제 2 테이블을 형성하고, 휴대용 단말기로 디지털 컨텐트를 공급할 수 있도록 하는 한쌍의 자격 인증 키 및 자격 인증 키 정보를 생성하여 송출한다.

휴대용 단말기 공급수단(20)은 상술한 권한부여수단(10)으로 등록 요청신호를 송출하고, 등록 요청신호에 의해 발생된 제조키 및 제조키 정보를 전송받는다.

컨텐트 공급부(30)는 상술한 권한부여수단(10)으로 등록 요청신호를 송출하고, 등록 요청신호에 의해 발생된 암호화된 디지털 컨텐트를 제공할 수 있는 자격이 부여되는 한쌍의 키와 그 키정보를 전송받고, 상술한 권한부여수단(10)의 제 2 테이블을 전송받는다.

PC(40)는 컨텐트 공급수단(30)에서 공급하는 디지털 컨텐트를 공급받아 재생, 출력시키고자 등록 요청신호를 컨텐트 공급수단(30)으로 송출하고, 상기 등록 요청신호에 의해 발생된 Public Key와 Public Key 정보를 전송받고, 휴대용 단말기(50)의 제조키 정보를 컨텐트 공급수단(30)으로 바이패스시키며, 제 2 테이블로부터 상기 제조키 정보에 해당되는 테이블 정보만 검출하여 암호화한 후 전송한다.

휴대용 단말기(50)는 상기 권한부여수단(10)에서 전송하는 제조키 및 제조키 정보를 입력받아 저장하고, PC(40)를 통해 컨텐트 공급수단(30)으로 제조키 정보를 송출하며, 상술한 PC(40)에서 전송되는 자신에게 해당하는 암호화된 제 2 테이블의

제조키 정보를 입력받아 저장한다.

이와 같이 구성된 본 발명에 따른 디지털 컨텐트 무단 복제 방지시스템의 동작을 첨부한 도면을 참조하여 좀 더 구체적으로 설명한다.

도 2에서 도 5는 도 1에 적용된 각 블록들이 등록요청 또는 디지털 컨텐트를 재생시키고자 하는 경우 이에 대한 키, 키정보 흐름을 설명하기 위한 도면이다.

도시된 바와 같이, 먼저 휴대용 단말기 공급수단(20)은 권한 부여 수단(10)에 제조한 휴대용 단말기(50)를 등록시키기 위한 등록 요청신호를 송출한다.

그러면, 권한부여수단(10)은 각 휴대용 단말기(50)가 고유하게 가질 수 있는 제조 키(MK_{Pd}) 및 제조 키 정보($Cert_{CA}(MK_{PD})$)를 생성하여 휴대용 단말기 공급수단(20)으로 전송한다.

그러므로 휴대용 단말기 공급수단(20)은 휴대용 단말기(50)를 제조하는 과정에서 권한부여수단(10)으로부터 부여받은 제조 키 및 그 제조 키 정보를 휴대용 단말기(50)의 템퍼리 레지스터 영역(tempery resistant area)에 다른 사용자가 알 수 없도록 저장시켜 놓는다.

한편, 권한부여수단(10)은 상술한 바와 같이 휴대용 단말기 공급수단(20)에 제공할 제조 키 및 제조키 정보를 생성함과 동시에 랜덤하게 토큰을 생성한다.

즉, 권한부여수단(10)은 두 개의 테이블을 가지고 있는데, 제 1 테이블은 권한부여수단(10)이 가지고 있는 테이블로서, 상술한 제조 키 및 제조 키 정보를 갖는 테이블이다.

한편, 제 2 테이블은 권한부여수단(10)이 컨텐트 공급수단(30)에게 전송해

주는 제조 키 정보 테이블(Manufacture Key Information Table)로서, 휴대용 단말기(50)의 ID(Identifier; 식별자), 제조 키에 의해 암호화된 토큰, 토큰에 대한 정보를 갖는 테이블이다.(첨부 도면 도 3참조)

이렇게 해서 상술한 휴대용 단말기 공급수단(20)에서 공급되는 휴대용 단말기(50)는 권한부여수단(10)에 암호화된 디지털 컨텐트를 다운로드받아 재생시킬 수 있는 권한을 부여 받은 것이다.

또한, 컨텐트 공급수단(30)도 휴대용 단말기 공급수단(20)과 마찬가지로 권한부여수단(10)으로부터 권한을 부여받아야 하는데, 그러기 위해서 컨텐트 공급수단(30)은 권한부여수단(10)에게 등록 요청 신호를 송출한다.

그러면 권한부여수단(10)와 컨텐트 공급수단(30) 사이에는 첨부 도면 도 2와 같이 키 및 키 정보가 생성된다.

즉, 컨텐트 공급수단(30)으로부터 등록요청신호를 입력받으면 권한부여수단(10)은 자신이 가지고 있는 Private Key 및 Public Key인 $PrvKey_{eph}$, $PubKey_{eph}$가 생성된다.

그리고, 컨텐트 공급수단(20)에 반영구적으로 남게 되는 상술한 바와 같이 한쌍의 키와 그 키정보인 {$PrvKey_{ISP}$, $PubKey_{ISP}$, $Cert_{CA}(PubKey_{isp})$}가 생성되고, 제조 키에 따라 두 개의 테이블이 생성된다.

그리고, 상술한 권한부여수단(10)과 컨텐트 공급수단(20)은 EC_DH(CA,ISP)로 생성되는 키를 채널 키로서 상호간에 공유하고, 공유한 채널 키에 의해 상호간에 채널이 안전하게 형성되므로 불법적인 사용자가 상술한 채널로부터 어떠한 정보도

다운로드할 수 없다.

한편, 권한부여수단(10)은 상술한 채널을 통해 생성시킨 키와 키정보를 공유키로 암호화한 후 컨텐트 공급수단(50)으로 전송한다. 그러면 권한부여수단(10)과 함께 공유하고 있는 키를 이용하여 전송된 정보를 해독시킨 후 컨텐트 공급수단(50)에 구비된 저장수단에 저장시킴으로써, 권한부여수단(10)과 컨텐트 공급수단(30) 사이의 셋업은 종료된다.

상술한 과정이 수행된 후 PC(40)가 컨텐트 공급수단(30)으로부터 암호화된 디지털 컨텐트를 다운로드받기 위해 등록요청신호를 송출한다. 그러면 컨텐트 공급수단(30)은 자신의 퍼블릭키와 퍼블릭 키정보인 $PubKey_{ISP}$, $Cert_{CA}(PubKey_{ISP})$를 PC(40)로 전송하고, PC(40)는 저장한다.

그리고, EC_DH(ISP, LCM)에 의해 발생된 키는 컨텐트 공급수단(30)과 PC(40)가 공유하는 채널 키로서, 컨텐트 공급수단(20)과 PC(40) 사이에 채널을 형성시키고, 이 채널로 안전하게 디지털 컨텐트를 전송 받을 수 있다.

또한, 컨텐트 공급수단(30)으로부터 PC(40)의 영구적인 Private Key, Public Key 한쌍이 채널을 통해 안전하게 공급되는데, 이로써 컨텐트 공급수단(30)과 PC(40)사이에서 안전하게 디지털 컨텐트를 다운로드 할 수 있는 시스템이 구현된다.

이때, 휴대용 단말기(50)로부터 PC(40)로 등록요청 신호가 입력되면 휴대용 단말기(50)는 권한부여수단(10)으로부터 제공받은 제조 키 정보를 컨텐트 공급수단(30)의 Public Key를 암호화한 후 PC(40)를 통해 컨텐트 공급수단(30)으로 전송한

다.

그러면 컨텐트 공급수단(30)은 전송된 암호화된 정보를 해독하고, 해독된 결과와 제 2 테이블이 가지고 있는 정보와 비교하여 일치하는 정보가 있는 경우 컨텐트 공급수단(30)은 테이블의 내용을 암호화한 후 PC(40)로 전송하고, PC(40)에서 해독하여 토큰을 얻어낸다.

이때, PC(40)에서 랜덤하게 채널 키(CK_{PD-LCM})가 생성되는데, 이 채널 키는 비밀이 유지될 수 있도록 생성된다. 이때 PC(40)에서 해독된 토큰을 이용하여 상술한 채널 키를 암호화한 후 휴대용 단말기(50)로 전송한다.

그러면, 휴대용 단말기(50)는 저장되어 있는 제조키를 이용하여 전송된 정보 중 컨텐트 공급수단(30)의 제 2 테이블에서 읽어들인 정보로부터 토큰 값을 읽어낸다.

그리고, 상술한 바와 같이 읽어낸 토큰 값을 이용하여 암호화된 정보를 해독시켜 채널 키를 얻어내어 저장함으로써, 채널 키를 PC(40)와 공유하게 된다. 이로써, 휴대용 단말기(50)의 등록과정은 끝나게 된다.

이렇게 하여 전체 시스템에서 서로 상호간에 암호화된 디지털 컨텐트를 전송받을 수 있는 권한을 모두 부여받게 된다.

마지막으로, PC(40)는 컨텐트 공급수단(30)으로부터 제공받은 디지털 컨텐트를 휴대용 단말기(50)로 다운로드 해줌에 있어, 무단 복제되는 것을 방지하기 위해 데이터 베이스를 가지고 있다. 이 데이터 베이스는 첨부도면 도 6에 도시된 바와 같이, RMS-DB로 명칭되어 있다.

상술한 데이터 베이스는 PC(40)와 휴대용 단말기(50) 사이에서 이루어지는 디지털 컨텐트 처리에 적용된다. 여기서, 데이터 베이스를 구성하고 있는 영역을 살펴보면, 먼저 디지털 컨텐트의 타이틀 또는 타이틀 ID 영역, 업데이트 토큰 정보(UTD) 영역, 디지털 컨텐트의 현상태에 대한 정보 영역, 재생 제어 정보 영역으로 이루어져 있다.

상술한 데이터 베이스는 PC(40)가 가지고 있는 비밀 키()에 의해 암호화된 형태로 PC(40)에 저장되어 있다. 상술한 내용 중에서 업데이트 토큰의 가장 중요한 특성은 PC(40)와 휴대용 단말기(50) 사이에서 휴대용 단말기(50)에 임의의 디지털 컨텐트를 다운로딩하거나, 또는 휴대용 단말기(50)로부터 PC(40)로 임의의 디지털 컨텐트를 업로딩할 때, 변화가 생기게 된다. 이때 변화된 업데이트 토큰은 휴대용 단말기(50)를 통해 다시 PC(40)로 전송되어 PC(40)에 저장된 업데이트 토큰을 갱신하게 된다.

처음에 PC(40)에서 디지털 컨텐트를 재생할 때마다 컨텐트 파일 포맷의 정보가 상술한 데이터 베이스 상에 새롭게 등록된다. 이렇게 데이터 베이스에 등록된 컨텐트는 매번 재생동작을 수행할 때마다 데이터 베이스를 참조하여 그 합법성을 체크해야 한다.

또한, PC(40)와 휴대용 단말기(50) 사이에서 디지털 컨텐트를 다운로드하거나, 또는 업로드할 경우 데이터 베이스의 세 번째 영역인 디지털 컨텐트의 현상태에 대한 정보 영역을 체크함으로써, 디지털 컨텐트를 상대방에게 복사형식으로 전송된 것인지, 아니면 컨텐트 자체가 전송되도록 할 것인지를 알 수 있다.

또한 체크 인/아웃을 체크함으로써, 디지털 컨텐트의 전송상태를 알 수 있다. 즉 체크 인경우는 디지털 컨텐트가 PC(40)에서 휴대용 단말기(50)로 다운로드되지 않았음을 알려주는 것이고, 체크 아웃인 경우는 PC(20)로부터 휴대용 단말기(50)로 디지털 컨텐트가 다운로드되는 상태이거나, 다운로드된 디지털 컨텐트가 다시 PC(40)로 업로드된 경우이다.

또한, 맨 마직막 영역은 재생 제어 정보 영역으로서, 재생회수에 대한 정보, 디지털 컨텐트 재생 만료기간, 디지털 컨텐트의 사면 기간에 대한 정보로 이루어져 있다.

즉, 상술한 바와 같이 디지털 컨텐트가 컨텐트 공급수단(30)으로부터 제공될 때 설정되어 있는 수치로서, 다운로드할 때마다 하나씩 다운카운트시켜 그 재생회수를 제어하는 것이다.

디지털 컨텐트 재생 만료기간은 재생 회수로 디지털 컨텐트의 재생, 출력상태를 제어하는 것이 아니라, 다운로드시 이미 설정된 재생 만료기간을 체크하여 그 기간동안만 디지털 컨텐트를 이용할 수 있도록 한 것으로서, 이 경우 재생 회수는 무관하다.

마지막으로 디지컬 컨텐트의 사면 기간으로서, 컨텐트 공급수단(30)이 가치가 떨어진 디지털 컨텐트에 대해서 그 재생회수나, 사용기간을 두지 않은 것으로서, 사용자가 컨텐트 공급수단(30)으로부터 상술한 디지컬 컨텐트를 다운로드받아 무한정 재생해 청취할 수 있다.

한편, 컨텐트 공급수단(30)이 PC(40)의 컨텐트 다운로드 요청을 수락하면,

먼저 PC(40)의 ID를 확인하고 나서, PC(40)로 소정의 파일 포맷을 갖는 컨텐트를 다운로드한다.

상술한 파일 포맷의 일 예를 첨부 도면 도 6에 의거해서 설명하면 다음과 같다.

본 발명이 지원하는 파일 포맷은 타이틀 ID 필드, 디지털 컨텐트의 작곡자, 가수, 레코드 라벨과 같은 정보를 갖는 컨텐트 디스크립션 필드, ECC, SNAKE, CODEC 등과 같은 알고리즘 식별 정보를 갖는 알고리즘 식별필드, 디바이스 ID, ISP_ID, LSP_ID, PD_ID와 같은 현재 정보가 출력되고 있는 소오스출력수단을 표시하는 SOI 필드, 복사 소유자 정보를 나타내는 카피라이트 홀더 인포메이션(COPYRIGHT HOLER INFORMATION; CHI) 필드, 라이트 매니지먼트 필드, 컨텐트 암호화 키 필드로 이루어져 있다.

여기서, SOI 필드의 ISP_ID는 본 발명의 컨텐트 공급수단(30)이며, LSP_ID는 PC(40)이며, PD_ID는 휴대용 단말기(50)이다.

상술한 포맷을 갖는 디지털 컨텐트를 다운로드 받아 재생하는 경우 PC(40)는 먼저 AIF 필드 또는 PH 필드로부터 암호화 알고리즘을 알아내고, 알아낸 암호화 알고리즘을 이용하여 SH 필드로부터 PC(40)의 Private Key를 복구시킨다.

그리고, PC(40)의 ID와 DEVICE-ID 필드에 있는 ID를 비교하여 일치하는지를 체크하고, RMF 정보로부터 복사 제어 상태, 재생 제어 상태 및 전송 제어 상태를 확인하여 그것을 PC(40)가 가지고 있는 데이터 베이스에 등록시킨다.

그리고 나서, CEK 필드를 이용하여 디지털 컨텐트 암호화 키를 회복시키고,

실제 디지털 컨텐트로 복귀시켜 재생할 수 있도록 한다.

PC(40)가 상술한 내용 중 어느 하나라도 위배하지 않을 경우 컨텐트 공급수단(30)은 PC(40)로 디지털 컨텐트를 다운로드 시킨다.

만약, RMF필드 중 특히, 재생 제어 상태를 변경할 필요는 경우라면, PC(40)는 데이터 베이스와 파일 포맷에 모두에서 재생 제어 상태 정보를 변경하고자 하는 정보로 대체시켜야 한다.

상술한 바와 같이 PC(40)에서 다운로드한 디지털 컨텐트를 다시 휴대용 단말기(50)로 다운로드 시켜 재생하고자 하는 경우 다음과 같은 절차를 거쳐야 한다.

먼저, PC(40)에서 휴대용 단말기(50)로 휴대용 단말기 ID와 휴대용 단말기(50)가 가지고 있는 UTD 정보를 요청한다.

그러면 휴대용 단말기(50)는 PC(40)의 채널 키(CK_{PD-LCM})로 UTD를 암호화한 후 휴대용 단말기 ID와 함께 PC(40)로 전송한다. 이때, PC(40)는 휴대용 단말기(50)로부터 전송된 정보를 확인한 후 휴대용 단말기 ID를 복귀시킴과 동시에 데이터 베이스 상에 있는 휴대용 단말기 ID와 비교하여 UTD와 SH 필드를 복귀시킨다.

만약, 상술한 UTD가 정확하나, RMF의 변경이 필요한 경우 PC(40)는 데이터 베이스와 파일 포맷 두군데를 모두 RMF 디지털 컨텐트로 갱신하여야 한다.

PC(40)는 새롭게 생성된 UTD로 데이터 베이스를 갱신시키고, 새롭게 생성된 UTD는 채널 키(CK_{PD-LCM})에 의해 암호화시킨 후 휴대용 단말기(50)로 전송된다.

만약, 전송 제어 상태는 'Transfer' 상태에서 디지털 컨텐트가 휴대용 단말기(50)로 전송되고 난 후 'Transferred'로 대체된다. 이때, PC(40)가 갖는 데이터

베이스에는 상술한 전송 제어 상태 필드가 파일 포맷으로 존재하지 않는다. 즉, 전송 제어 상태필드는 'Transfer', 'Transferred', 'Transfer-non'와 같은 세가지 형태를 갖는다.

한편, 복사 제어 상태는 맨처음 체크인(Check-in)으로 지칭되고, 디지털 컨텐트가 전송되고 난 후 PC(40)가 가지고 있는 데이터 베이스와 파일 포맷 상에서 체크 아웃(Check-out)으로 대체된다.

만약 복사 제어 상태 필드가 '복사 불가(Copy-never)'로 지칭되어 있으면, PC(40)의 디지털 컨텐트는 휴대용 단말기(50)로 다운로드되지 않는다.

상술한 과정 중 하나라도 위배하지 않을 경우 휴대용 단말기(50)로 디지털 컨텐트가 다운로드 된다.

시스템에서는 마지막 단계라고 볼 수 있는 휴대용 단말기(50)로부터 저장매체(60)로 디지털 컨텐트를 처리하는 방법에 대해서 간단히 설명하면 다음과 같다.

첫째, 각 휴대용 저장매체(60)에 고유 ID가 존재하는 경우, 휴대용 단말기(50)에서 저장매체(60) 상에 디지털 컨텐트를 기록하기 위해, 단지 저장매체(60) 상에 컨텐트를 기록하고, 기록한 디지털 컨텐트를 시크리트 헤더(Secret Header)로 복귀하고, 암호화 키로서 저장매체(60) 상에 존재하는 저장매체의 고유 ID를 이용하여 디지털 컨텐트를 다시 암호화한다.

둘째, 각 저장매체(60)에 고유 ID가 존재하지 않는 경우, 휴대용 단말기(50)에서 저장매체(60) 상에 디지털 컨테트를 기록하기 위해, 단지 저장매체(60) 상에 컨텐트를 기록하고, 기록한 디지털 컨텐트를 시크리트 헤더(Secret Header)로 복귀

하고, 랜덤하게 발생되는 키를 이용하여 다시 암호화한다.

여기서, 랜덤하게 발생되는 키인 T는 일반적인 시크리트 키인 S에 의해 암호화된다. 이때 일반적인 시크리트 키인 S는 휴대용 단말기의 제조자에 의해 미리 설정되어 있다.

그리고, 상기 암호화된 T는 저장매체(60)의 히든 영역에 기록된다.

상술한 바와 같이 첫 번째 경우, 저장매체(60) 내에 있는 모든 디지털 컨텐트는 모든 휴대용 단말기(50)에서 재생시킬 수 있다. 그러나, 두 번째 경우 저장매체(60) 내에 있는 모든 컨텐트는 오직 이 시스템에 채택된 제조자에 의해 생산된 휴대용 단말기에 의해서만 재생시킬 수 있다.

본 발명에서 언급된 디지털 컨텐트는 임의의 휴대용 단말기 뿐만 아니라 임의의 PC로 업로드시킬 수 있다.

본 발명은 전송 제어 상태 필드를 PC(40)가 갖는 데이터 베이스와 파일 포맷 내에 모두 가지고 있다. 본 발명은 디지털 컨텐트를 PC(40)에서 휴대용 단말기(50)로 다운로드시킬 뿐만 아니라, 휴대용 단말기(50)에서 PC(40)로 업로드시킬 수 있도록 지원한다.

만약, 디지털 컨텐트의 필드에 'transfer'이 표시되어 있다면 디지털 컨텐트를 휴대용 단말기(50)로 다운로드 시키고, PC(40)의 데이터 베이스의 관계되는 필드는 'transfer'에서 'transferred' 표시로 대체되고, 그 변경된 정보를 휴대용 단말기(50)로 다운로드한다.

그리고, 휴대용 단말기(50)에 다운로드된 디지털 컨텐트는 다시 PC(40)로 업

로드되기 전까지는 PC(40) 상에서 재생시킬 수 없다. 그러나, 저장매체(60)에서 다운로드된 디지털 컨텐트는 임의의 휴대용 단말기(50)에서 재생시킬 수 있다. 휴대용 단말기(50)를 경우에서 또다른 PC(40)로 업로드시킬 수 있다.

또한, 본 발명이 적용된 PC(40)나, 휴대용 단말기(50)에는 매우 다양한 입력장치가 부가적으로 연결될 수 있는데, 첨부 도면 도 7에 도시된 바와 같이, PC(40) 및 휴대용 단말기(50)에 부가적으로 연결되는 입력장치로는 RedBook CD, 오디오 CD, 슈퍼 오디오 CD, DVD Disk 및 아날로그 장치 등이 있다.

첨부 도면 도 8은 상술한 도7에 도시된 출력소오스(Outsourse)의 입력 제어를 설명하기 위한 도면이다.

도시된 바와 같이, API(응용 프로그램 인터페이스)는 입력이 본 발명이 지원하는 시스템에 합법적으로 인증된 것인지를 확인하고, 아울러 입력을 본 발명에서 지원하는 파일 포맷으로 전환하기 위해 필요한 정보를 추출하는 역할을 한다.

상술한 입력의 인증 확인은 입력장치의 정보가 수위표를 가질 경우, 상술한 API는 그것을 탐지할 수 있어야 한다. 또한, 입력장치의 정보가 암호화된 형태를 가질 경우 상술한 API는 암호화키와 암호화 알고리즘을 추출할 수 있어야 할 뿐만 아니라 입력장치의 정보가 암호화된 형태를 가질 경우 API는 입력장치의 정보를 포함하는 저장매체에 기록 포맷의 인증 여부를 확인해야 한다.

상술한 API가 입력 제어 층(Import control layer)으로 전달되기 위해 필요한 정보는 저장매체의 종류에 대한 정보, 예를 들면 오디오 CD, DVD 오디오 등이 있다. 또한, 입력되는 디지털 컨텐트의 초기형태에 대한 정보인 디지털 컨텐트에

대한 정보, 예를 들면 타이틀, 플레이어, 가수 등이다.

그리고, 암호화 알고리즘에 대한 정보인 암호화 키에 대한 정보는 휴대용 단말기의 입력 제어에서 이 입력 제어 층은 인증된 입력 API로부터 일정량의 정보를 받아서 입력 컨텐트를 아래에 열거한 규칙에 따라서 본 발명에서 지원하는 파일 포맷에 맞도록 재 구성한다.

복사 제어 상태 즉, '복사불가' 표시, 혹은 '체크 인/체크 아웃(선택적으로)', 재생 제어 상태 즉, '재생회수=무한정 혹은 횟수(선택적)', 전송 제어 상태 즉, '전송불가'표시, 'LCM_ID'를 SOI 필드와 시크리트 헤더의 디바이스 ID 필드로 표시된다.

만약에, 입력되는 디지털 컨텐트가 암호화되어 있지 않을 경우 랜덤하게 키를 생성하여 그것을 키에 의해 암호화한다. 즉, 입력되는 디지털 컨텐트가 휴대용 단말기와 다른 종류의 암호화 알고리즘에 의하여 암호화된 형태를 가질 경우 이 층은 휴대용 단말기에 재생되는 컨텐트를 **전환-암호화(Trans-encryption)**한다.

그리고, PC가 가지고 있는 Public Key에 의해 시크리트 헤더부분을 Public Key로 암호화한다.

또한, 본 발명에 적용되는 휴대용 단말기의 인터페이스 층은 휴대용 단말기가 정확한 ID와 시크릿 채널 키를 가지는지의 여부를 체크함으로써 연결된 휴대용 단말기를 인증한다.

한편, 상술한 휴대용 단말기로 입력되는 아날로그 입력은 PDFM 내에서의 입력 제어 층은 아래 열거한 규칙에 따라 아날로그 입력으로부터 본 발명에서 지원하

는 압축 디지털 컨텐트를 만든다.

즉, 아날로그 입력의 각 프레임이 수신되자마자 입력 제어 흥은 먼저 그 프레임을 인코딩하고, 랜덤하게 발생된 키를 사용하여 인코딩된 프레임을 암호화한다. 만약 모든 프레임이 암호화되었다면 다음 단계를 따른다.

복사 제어 상태 즉, '복사불가' 표시, 혹은 '체크 인/체크 아웃(선택적으로)', 재생 제어 상태 즉, '재생회수=무한정 혹은 횟수(선택적)', 전송 제어 상태 즉, '전송불가'표시, PD_ID를 SOI 필드와 시크리트 헤더의 디바이스-ID로 표시한다.

상술한 휴대용 단말기는 자신이 갖는 채널 키에 의해 시크리트 헤더를 암호화한다. 즉, 아날로그 입력으로부터의 전환된 경우 본 발명에서 지원하는 디지털 컨텐트가 "PD-ID"로 표시된 시크리트 헤더의 SOI 필드를 가질 경우, 저장매체에 디지털 컨텐트를 기록할 경우 저장매체의 고유 ID를 사용하지 않는다. 이것은 휴대용 단말기로 입력되는 아날로그 입력은 휴대성을 갖지 못한다는 것을 뜻한다.

마지막으로 출력소오스 장치 중 하나인 키오스크는 CD-ripping에서 저장매체로 전송되는 본 발명에서 지원하는 디지털 컨텐트를 만들어 파는 기계나 상점으로 볼 수 있다.

여기서, 우리는 키오스크류의 기계를 저장매체의 인터페이스를 지닌 특별한 PC로 간주한다. 여기서 저장매체 인터페이스는 저작권 소유자와 디지털 컨텐트 공급수단만이 특별 계약을 통해 사용할 수 있다.

이와 같은 목적을 달성하기 위한 본 발명에 따른 ~~RGLCM을를~~ 통해 디지털 컨텐트 공급수단으로부터 공급되는 암호화된 디지털 컨텐트를 입력받아 휴대용 저장매체로 전송해주는 휴대용 단말기를 갖는 복제 방지 시스템에 있어서(**LCM에서 직접 휴대용 저장매체로 저장할 수도 있음**), 블랑섹터의 물리적 주소, **PD (또는 LCM)에서 발생하여 저장매체의 키영역(Spare Area)에 저장한** 랜덤한 수 및 ~~RGLCM~~에서 생성하여 전송되는 ~~시크릿~~ 키를 입력으로 받아 함수처리하고, 함수 처리된 결과값으로 디지털 컨텐트의 헤더를 암호화하여 송출하는 휴대용 단말기와, 상기 휴대용 단말기로 블랑섹터의 물리적 주소를 읽어들여 전송하고, 휴대용 단말기에서 랜덤하게 발생되는 수를 키 값으로 저장하며, 휴대용 단말기를 통해 입력되는 암호화된 디지털 컨텐트 및 함수 결과값에 의해 다시 암호화된 헤더 정보를 섹터 데이터로 저장하는 휴대용 저장매체를 포함한다.

이하, 첨부한 도면들을 참조하여 본 발명의 바람직한 실시 예를 상세히 기술하기로 한다.

도 1은 본 발명인 무단 복제를 방지하기 위한 휴대용 저장매체를 갖는 시스템을 도시한 블록도로서, 그 구성은 다음과 같다.

휴대용 단말기(100)는 불량섹터의 물리적 주소, PD (또는 LCM)에서 발생하여 저장매체의 키영역(Spare Area)에 저장한 랜덤한 수 및 PCLCM에서 생성하여 전송되는어 휴대용 단말기에 안전하게 저장된 시크릿트 채널 키를 입력으로 받아 함수처리하고, 함수 처리된 결과값으로 디지털 컨텐트의 헤더를 암호화하여 송출한다.

상술한 휴대용 단말기(100)는 MP3 음악 파일을 다운로드받아 재생시킬 수 있는 기기이다.

저장매체(200)는 상기 휴대용 단말기(100)로 불량섹터의 물리적 주소를 읽어들여 전송하고, 휴대용 단말기(100)에서 랜덤하게 발생되는 수를 리턴값 f 함수의 입력 인자의 일부로써 키영역(Spare Area)으로 저장하며, 휴대용 단말기를 통해 입력되는 암호화된 디지털 컨텐트 및 함수 결과값에 의해 다시 암호화된 헤더 정보를 섹터 데이터로 저장한다.

상술한 저장매체(200)는 스마트 미디어를 포함한 일반적인 저장매체 이다.

이와 같이 구성된 본 발명에 따른 무단 복제를 방지하기 위한 휴대용 저장매체를 갖는 시스템의 동작을 첨부한 도면을 참조하여 좀 더 구체적으로 설명한다.

먼저, 휴대용 단말기(100)는 PCLCM로부터 디지털 컨텐트를 다운로드 받거나 직접 컨텐트 공급수단으로부터 다운로드 받는다.

이때, 휴대용 단말기(100)는 PCLCM으로부터 휴대용 단말기(100)와 PCLCM 사이에 안전한 채널을 형성시키기 위해 휴대용 단말기(100) 및 PCLCM는 하나의 시크리트 키(secret key, S-Channel Key, CK)를 공유하게 된다.

그리고, 휴대용 단말기(100)의 입력포트를 통해 암호화된 디지털 컨텐트를

입력받아 저장매체(200)로 전송시켜 저장매체(200)의 섹터 데이터 영역에 저장되도록 한다.

그리고 휴대용 단말기(100)는 다운로드 받은 디지털 컨텐트가 저장매체(200)를 통해 불법 복제되는 것을 방지하기 위해 디지털 컨텐트의 헤더부분을 다시 한번 암호화시킨다. **(원래, 디지털 컨텐트의 헤더부분은 CK로 암호화되어 LCM에서 휴대용 단말기로 전송된다.)** 이때, 암호화 하는 키를 발생시키는 것이 함수처리수단(110)이다.

즉, 상술한 함수처리수단(110)은 저장매체(200)에서 전송하는 불량섹터의 물리적 주소를 입력으로 받는 한편, 휴대용 단말기(100)의 랜덤발생수단(120)을 통해 발생한 랜덤한 수를 입력받는다. 이때 발생된 랜덤한 수는 저장매체(200)의 키영역에도 전송되어 저장된다.

그러므로, 함수처리수단(110)은 상술한 불량섹터의 물리적 주소, 랜덤한 수 및 ~~PG~~LCM에서 생성한 공유 키를 입력받아 함수 처리하고, 그 결과값을 해독 **및 암호** 수단(130)으로 입력하여 디지털 컨텐트의 헤더부분을 다시 암호화시켜 저장매체(200)의 섹터 데이터 영역에 저장시킨다.

이때, 함수처리수단(120)으로 입력되는 불량섹터의 물리적 주소, 랜덤한 수 및 공유 키는 모두 입력받을 수도 있고, 그 중에 하나만 선택적으로 입력받아 함수처리하여 디지털 컨텐트의 헤더를 암호화할 수 있다.

【발명의 효과】

따라서, 상술한 바와 같이 본 발명은 전체 시스템이 서로 상호간에 통신을 수행하는 수단끼리 채널 키를 공유하고 안전한 채널을 형성시켜 상호간에 디지털 컨텐트를 주고 받음으로써, 중간에 불법 사용자가 디지털 컨텐트를 가져갈 수 없도록 할뿐만 아니라, 합법적인 사용자가 합법적으로 다운로드받은 디지털 컨텐트라 하더라도 휴대용 단말기도 상술한 구성을 갖고 있기 때문에 상호간에 무단으로 복제되는 것을 방지할 수 있다는 효과를 제공한다.

따라서, 상술한 바와 같이 본 발명은 디지털 컨텐트가 저장된 저장매체~~인 스마트 미디어~~를 데드 카피(DEAD COPY)하여 디지털 컨텐트를 복제하더라도 재생시킬 수 없기 때문에 불법적으로 복제하는 것을 근본적으로 방지할 수 있다는 효과를 제공한다.

PATENT
P55690

What is claimed is:

【청구항 1】

암호화 알고리즘에 의해 암호화된 디지털 컨텐트를 전송받아 해독한 후 재생, 출력할 수 있는 디지털 컨텐트 복제 방지 시스템에 있어서,

상기 암호화된 디지털 컨텐트를 공급하거나, 또는 공급받아 재생, 출력할 수 있도록 제조키 및 제조키 정보를 생성, 송출하고, 디지털 컨텐트를 제공할 수 있는 인증 자격 키 및 그 키정보를 암호화하여 송출하는 권한부여수단;

상기 권한부여수단으로 등록 요청신호를 송출하고, 등록 요청신호에 의해 발생된 제조키 및 제조키 정보를 전송받는 휴대용 단말기 공급수단;

상기 권한부여수단으로 등록 요청신호를 송출하고, 등록 요청신호에 의해 발생된 암호화된 디지털 컨텐트를 제공할 수 있는 자격을 부여하기 위해 권한부여수단에서 생성된 한쌍의 키와 그 키정보를 전송받는 컨텐트 공급수단; 및

상기 컨텐트 공급수단에서 공급하는 디지털 컨텐트를 공급받아 재생, 출력시키고자 등록 요청신호를 컨텐트 공급수단으로 송출하고, 상기 등록 요청신호에 의해 발생된 퍼블릭키와 퍼블릭키 정보 및 디지털 컨텐트를 공급받을 수 있도록 암호화된 한쌍의 키와 그 키정보를 전송받는 PC로 이루어진 것을 특징으로 하는 디지털 컨텐트 무단 복제 방지 시스템.

【청구항 2】

제 1 항에 있어서, 상기 권한부여수단과 컨텐트 공급수단은, 비밀 채널을 형성하기 위한 제 1 공유키를 생성하고, 상기 권한부여수단에서 컨텐트 공급수단으로

공급되는 키 및 키정보는 상기 제 1 공유키에 의해 암호화된 후 컨텐트 공급수단으로 전송되도록 하는 것을 특징으로 하는 디지털 컨텐트 무단 복제 방지 시스템.

【청구항 3】

제 1 항에 있어서, 상기 컨텐트 공급수단은, 상기 권한부여수단과 동일하게 갖는 제 1 공유키를 이용하여 권한부여수단으로부터 전송된 키 및 키정보를 해독한 후 저장시키는 것을 특징으로 하는 디지털 컨텐트 무단 복제 방지 시스템.

【청구항 4】

제 1 항에 있어서, 상기 컨텐트 공급수단과 PC는 비밀 채널을 형성시키기 위해 제 2 공유키를 형성시키고, 컨텐트 공급수단은 제 2 공유키를 이용하여 PC로 전송하는 키 및 키정보를 암호화하며, PC는 컨텐트 공급수단과 공유한 제 2 공유키를 이용하여 키 및 키정보를 해독한 후 저장하는 것을 특징으로 하는 디지털 컨텐트 복제 방지 시스템.

【청구항 5】

암호화 알고리즘에 의해 암호화된 디지털 컨텐트를 전송받아 해독한 후 재생, 출력할 수 있는 디지털 컨텐트 복제 방지 시스템에 있어서,

상기 암호화된 디지털 컨텐트를 공급하거나, 또는 공급받아 재생, 출력할 수 있도록 제조키, 제조키 정보 및 상기 제조키와 제조키 정보를 갖는 제 1 테이블을 형성하고, 상기 테이블과 한쌍으로 휴대용 단말기의 ID, 제조키로 토큰을 암호화시킨 정보, 토큰을 갖는 제 2 테이블을 형성하고, 휴대용 단말기로 디지털 컨텐트를 공급할 수 있도록 하는 한쌍의 자격 인증 키 및 자격 인증 키정보를 생성하여 송출

하는 권한부여수단;

상기 권한부여수단으로 등록 요청신호를 송출하고, 등록 요청신호에 의해 발생된 제조키 및 제조키 정보를 전송받는 휴대용 단말기 공급수단;

상기 권한부여수단으로 등록 요청신호를 송출하고, 등록 요청신호에 의해 발생된 암호화된 디지털 컨텐트를 제공할 수 있는 자격이 부여되는 한쌍의 키와 그 키정보를 전송받고, 상기 권한부여수단의 제 2 테이블을 전송받는 컨텐트 공급수단;

상기 컨텐트 공급수단에서 공급하는 디지털 컨텐트를 공급받아 재생, 출력시키고자 등록 요청신호를 컨텐트 공급수단으로 송출하고, 상기 등록 요청신호에 의해 발생된 퍼블릭키와 퍼블릭키 정보를 전송받고, 제조키 정보를 컨텐트 공급수단을 바이패스 시키며, 제 2 테이블로부터 상기 제조키 정보에 해당되는 테이블 정보를 검출하여 암호화한 후 전송하는 PC; 및

상기 권한부여수단에서 전송하는 제조키 및 제조키 정보를 입력받아 저장하고, PC를 통해 컨텐트 공급수단으로 제조키 정보를 송출하며, 상기 PC에서 전송되는 자신에게 해당하는 암호화된 제 2 테이블의 제조키 정보를 입력받는 휴대용 단말기로 이루어진 것을 특징으로 하는 디지털 컨텐트 무단 복제 방지 시스템.

【청구항 6】

제 5 항에 있어서, 상기 휴대용 단말기에 장착되어 컨텐트 공급부로부터 공급되는 디지털 컨텐트를 휴대용 단말기를 통해 전송받아 저장하는 저장매체를 더 포함하는 것을 특징으로 하는 디지털 컨텐트 복제 방지 시스템.

【청구항 7】

제 5 항에 있어서, 상기 권한부여수단과 컨텐트 공급수단은, 시크리트 채널을 형성하기 위한 제 1 공유키를 생성하고, 상기 권한부여수단에서 컨텐트 공급수단으로 공급되는 키 및 키정보는 상기 제 1 공유키에 의해 암호화된 후 컨텐트 공급수단으로 전송되도록 하는 것을 특징으로 하는 디지털 컨텐트 무단 복제 방지 시스템.

【청구항 8】

제 5 항에 있어서, 상기 컨텐트 공급수단은, 상기 권한부여수단과 동일하게 갖는 제 1 공유키를 이용하여 권한부여수단으로부터 전송된 키 및 키정보를 해독한 후 저장시키는 것을 특징으로 하는 디지털 컨텐트 무단 복제 방지 시스템.

【청구항 9】

제 5 항에 있어서, 상기 컨텐트 공급수단과 PC는 시크리트 채널을 형성시키기 위해 제 2 공유키를 형성시키고, 컨텐트 공급수단은 제 2 공유키를 이용하여 PC로 전송하는 키 및 키정보를 암호화하며, PC는 컨텐트 공급수단과 공유한 제 2 공유키를 이용하여 키 및 키정보를 해독한 후 저장하는 것을 특징으로 하는 디지털 컨텐트 무단 복제 방지 시스템.

【청구항 10】

제 5 항에 있어서, 상기 토큰은 권한부여수단에 의해 랜덤하게 발생되는 것을 특징으로 하는 디지털 컨텐트 무단 복제 방지 시스템.

【청구항 11】

제 7 항에 있어서, 상기 PC는 휴대용 단말기와 시크리트 채널을 형성시키기 위해 채널 키를 랜덤하게 발생시켜 암호화시킨 후 휴대용 단말기로 전송하고, 휴대용 단말기는 PC로부터 전송된 채널 키를 해독시켜 PC와 공유할 수 있도록 저장하는 것을 특징으로 하는 디지털 컨텐트 무단 복제 방지 시스템.

【청구항 12】

제 7 항 또는 제 11 항에 있어서, 상기 휴대용 단말기에서 암호화된 제 2 데이블은, 휴대용 단말기에 저장된 제조키를 이용하여 해독시켜 토큰을 알아내고, 상기 토큰을 이용하여 PC와 공유하는 채널키를 해독시켜 저장하는 것을 특징으로 하는 디지털 컨텐트 무단 복제 방지 시스템.

【청구항 13】

PC에서 휴대용 단말기로 디지털 컨텐트를 다운로드 받거나, 휴대용 단말기에서 PC로 디지털 컨텐트를 업로드하는 디지털 컨텐트 복제 방지 시스템에서,

상기 PC는, 디지털 컨텐트가 무단 복제되는 것을 방지하기 위해 디지털 컨텐트의 합법성을 체크하는데 필요한 정보를 갖는 데이터 베이스를 가지고, 상기 데이터 베이스는 PC에 의해 랜덤하게 발생되는 채널 키에 의해 암호화되거나, 암호화된 정보를 해독하여 데이터 베이스가 가지는 정보와 비교하여 디지털 컨텐트의 무단복제여부를 판단하고,

상기 휴대용 단말기는, 상기 PC로부터 전송되는 암호화된 정보를 PC와 공유하는 채널 키를 이용하여 해독한 후 토큰을 업데이트하고, 업데이트된 토큰을 암호화한 후 상기 PC로 전송하는 것을 특징으로 하는 디지털 컨텐트 무단 복제 방지 시

스템.

【청구항 14】

제 13 항에 있어서, 상기 데이터 베이스는, 디지털 컨텐트의 타이틀 ID, 업데이트 토큰 정보 영역, 디지털 컨텐트의 현상태에 대한 정보 영역, 재생 제어 정보 영역으로 나누어짐을 특징으로 하는 디지털 컨텐트 무단 복제 방지 시스템.

【청구항 15】

제 14 항에 있어서, 디지털 컨텐트의 현상에 대한 정보 영역은, 복사, 전송 및 디지털 컨텐트의 다운로드 또는 업로드 여부를 알 수 있도록 구성되어 있음을 특징으로 하는 디지털 컨텐트 무단 복제 방지 시스템.

【청구항 16】

제 14 항에 있어서, 디지털 컨텐트 재생 제어 정보 영역은, 재생회수에 대한 정보, 디지털 컨텐트 재생 만료기간, 디지털 컨텐트의 사면 기간에 대한 정보로 구성되어 있음을 특징으로 하는 디지털 컨텐트 무단 복제 방지 시스템.

【청구항17】

~~PGLCM을~~를 통해 디지털 컨텐트 공급수단으로부터 공급되는 암호화된 디지털 컨텐트를 입력받아 휴대용 저장매체로 전송해주는 휴대용 단말기를 갖는 복제 방지 시스템에 있어서, **(LCM에서 직접 휴대용 저장매체로 저장할 수도 있음)**

볼륨섹터의 물리적 주소, 랜덤한 수 및 ~~PGLCM~~에서 생성하여 전송되는 시크리트 키를 입력으로 받아 함수처리하고, 함수 처리된 결과값으로 디지털 컨텐트의 헤더를 암호화하여 송출하는 휴대용 단말기; 및

상기 휴대용 단말기로 볼륨섹터의 물리적 주소를 읽어들여 전송하고, 휴대용 단말기에서 랜덤하게 발생되는 수를 키 값으로 저장하며, 휴대용 단말기를 통해 입력되는 암호화된 디지털 컨텐트 및 함수 결과값에 의해 다시 암호화된 헤더 정보를 섹터 데이터로 저장하는 휴대용 저장매체로 이루어짐을 특징으로 하는 무단 복제를 방지하기 위한 휴대용 저장매체를 갖는 시스템.

COPY PROTECTION SYSTEM

FOR PORTABLE STORAGE MEDIA

ABSTRACT

【요약】

사용자가 재생하고자 다운받은 암호화된 디지털 컨텐트가 무단 복제되는 것을 방지하기 위해 사용자와 연결되는 모든 시스템이 서로 상호간에 공유할 수 있는 다수의 키를 생성하여 공유하고, 상호간에 형성된 시크리트 채널를 이용하여 디지털 컨텐트를 다운로드 또는 업로드하는 디지털 컨텐트 무단 복제 방지 시스템이 개시되어 있다.

디지털 컨텐트를 공급하는 수단이 권한부여수단으로부터 합법적으로 디지털 컨텐트를 공급할 수 있다는 권한을 부여받는다. 그리고 PC는 상기 디지털 컨텐트 공급수단으로부터 인증을 받으며, 이때 디지털 컨텐트 공급수단과 PC는 공유키를 형성하여 둘 사이에 시크리트 채널을 형성한다. 그리고, 휴대용 단말기는 PC를 통해 디지털 컨텐트 공급수단으로부터 인증을 받으며, PC와 휴대용 단말기는 채널 키에 시크리트 채널을 형성한다. 그리고 PC와 휴대용 단말기에 사이에 디지털 컨텐트를 각각이 가지고 있는 제어 상태에 따라 다운로드 또는 업로드되도록 한다. 따라서, 디지털 컨텐트 공급수단, PC 및 휴대용 단말기 사이에서 전송되는 디지털 컨텐트의 무단으로 복제하는 불법 복제를 방지할 수 있다는 효과가 있다.

휴대용 저장매체 제조시 발생되는 불량섹터의 물리적 주소를 이용하여 휴대용 저장매체에 저장되는 암호화된 디지털 컨텐트의 헤더를 다시 암호화시켜 휴대용 단말기 **또는 LCM을** 통해 다운로드받은 디지털 컨텐트를 저장매체를 통해 불법으로 복제할 수 없도록 하는 무단 복제를 방지하기 위한 휴대용 저장매체를 갖는 시스템이 개시되어 있다. 불량섹터의 물리적 주소, 랜덤한 수 및 **LCM**에서 생성하여 전송되는 시크리트 키를 입력으로 받아 함수 처리하고, 함수 처리된 결과값으로 디지털 컨텐트의 헤더를 암호화하여 송출하는 휴대용 단말기와, 상기 휴대용 단말기로 불량섹터의 물리적 주소를 읽어들여 전송하고, 휴대용 단말기에서 랜덤하게 발생되는 수를 키 값으로 **하여 저장매체의 키영역(일명, Spare Area라고도 함)** 저장하며, 휴대용 단말기를 통해 입력되는 암호화된 디지털 컨텐트 및 함수 결과값을 이용하여 암호화된 헤더 정보를 저장하는 휴대용 저장매체를 포함한다. 따라서, 디지털 컨텐트가 저장된 저장매체~~인 스마트 미디어~~(**스마트미디어로 국한 시키지 말것**)를 데드 카피(DEAD COPY)하여 디지털 컨텐트를 복제하더라도 재생시킬 수 없기 때문에 불법적으로 복제하는 것을 근본적으로 방지할 수 있다는 효과가 있다.